UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/531,173	04/11/2005	Kan Torii	00862.023417	5079

5514 7590 01/29/2008
FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
PACHURA, REBECCA L	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
01/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/531,173	**Applicant(s)** TORII, KAN	
	Examiner Rebecca L. Pachura	**Art Unit** 4171	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 April 2005* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *10/17/2005, 11/07/2006*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. **Claims 1-19 are presented for examination.**

The claims and only the claims form the metes and bounds of the invention. "Office personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969)" (MPEP p 2100-8, c 2, I 45-48; p 2100-9, c 1, l 1-4). The Examiner has full latitude to interpret each claim in the broadest reasonable sense. The Examiner will reference prior art using terminology familiar to one of ordinary skill in the art. Such an approach is broad in concept and can be either explicit or implicit in meaning.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 11/07/2006 and 10/17/2005 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Preliminary Amendment

3. The Preliminary Amendment submitted on 06/22/2005 is duly noted and "Entered".

Priority

4. The claim for Foreign Priority, application # 2003-021039 filed in Japan on January 29, 2003 is duly noted.

Claim Objections

5. Claims 3-6, 9-12, 14-15, 17-18 are objected to because of the following informalities: They all start the sentence with *"An"* and they should be *"The"*. Claim 11, line 1 states *"to any one of claim 7"* it should state *"to claim 7"*. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. **Claim 19 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.** *"A program"* must be tangibly embodied in something. In view of the below sited MPEP section the claims are non-statutory because they are functional descriptive material per se.

> **MPEP 2106.01 [R-5]**
> Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).)
> Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se, 33 F.3d at 1360, 31 USPQ2d at 1759.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. **Claims 1, 2, 5, 6, 7, 8, 11, 12, 13, 14, 16, 17, and 19 rejected under 35 U.S.C. 102(b) as being anticipated by US 6021496 (Dutcher) (Applicant's IDS).**

As to claim 1, Dutcher discloses an authentication apparatus having a plurality of authentication mechanisms, comprising: an input unit adapted to input authentication information of an object of authentication (Dutcher column 5, lines 5-8: In this known technique, a user seeking to be authenticated at the client simultaneously presses the "control", "alt" and "delete" keys of the keyboard to initiate a logon session);

a determination unit adapted to determine whether the authentication information that has been input by said input means is that of an object of authentication that is capable of changing over the plurality of authentication mechanisms (Dutcher column 2, lines 55-64: This enables the user to set up his or her own desktop appearance and preferences, irrespective of where in the network the user logs on. The preferences may include a set of access rights vis-a-vis information retrieved from the server. After the user completes his or her work, the dynamically-established user account may be maintained, disabled or deleted from the client);

a display control unit adapted to display a list of the plurality of authentication mechanisms if it has been determined by said determination unit that the object of authentication is one capable of making the changeover (Dutcher column 3, lines 8-15: If desired, the administrator may then apply a discovery "policy" to tailor the way in which a user may access and interact with the discovered information. Then, when a user attempts to logon, the list(s) (as originally compiled or as modified via what the particular discovery policy allows) are presented to the user to enable the user to select the location(s) at which he or she is to be authenticated);

and a registration unit adapted to register, as an effective authentication mechanism, an authentication mechanism that has been selected from the list displayed by said display control unit (Dutcher column 3, lines 16-23: Following successful authentication, a user account is dynamically established at the client by retrieving from the server user information and a set of "group" privileges associated with the authenticated user. A local representation of these privileges is then dynamically created on the client, after which the privileges are linked to the user account to make the user a member of the local representation. In this manner, the group information is saved on the local machine and the authenticated user is afforded appropriate access rights to the client and the server. The user may download his or her "user profile" to instantiate a particular desktop representation or other user preference so that the user consistently sees what he or she expects to see when logging on to the client).

As to claim 2, Dutcher discloses an authentication apparatus having a plurality of authentication mechanisms, comprising: an input unit adapted to input authentication information of an object of authentication (Dutcher column 5, lines 5-8: In this known technique, a user seeking to be authenticated at the client simultaneously presses the "control", "alt" and "delete" keys of the keyboard to initiate a logon session);

a determination unit adapted to determine whether the authentication information that has been input by said input unit is that of an object of authentication that is capable of changing over the plurality of authentication mechanisms (Dutcher column 2, lines 55-64: This enables the user to set up his or her own desktop appearance and preferences, irrespective of where in the network the user logs on. The preferences may include a set of access rights vis-a-vis information retrieved from the server. After the user completes his or her work, the dynamically-established user account may be maintained, disabled or deleted from the client);

a display control unit adapted to display a list of the plurality of authentication mechanisms if it has been determined by said determination unit that the object of authentication is one capable of making the changeover (Dutcher column 3, lines 8-15: If desired, the administrator may then apply a discovery "policy" to tailor the way in which a user may access and interact with the discovered information. Then, when a user attempts to logon, the list(s) (as originally compiled or as modified via what the particular discovery policy allows) are presented to the user to enable the user to select the location(s) at which he or she is to be authenticated);

a selection unit adapted to permit selection of an authentication mechanism in the list displayed by said display control unit (Dutcher column 3, lines 10-15: Then, when a user attempts to logon, the list(s) (as originally compiled or as modified via what the particular discovery policy allows) are presented to the user to enable the user to select the location(s) at which he or she is to be authenticated);

and a registration unit adapted to register the authentication mechanism, which has been selected by using said selection unit, as an effective authentication mechanism in a case where the authentication mechanism that has been selected using said selection unit has registered authentication information input by said input unit (Dutcher column 3, lines 16-23: Following successful authentication, a user account is dynamically established at the client by retrieving from the server user information and a set of "group" privileges associated with the authenticated user. A local representation of these privileges is then dynamically created on the client, after which the privileges are linked to the user account to make the user a member of the local representation. In this manner, the group information is saved on the local machine and the authenticated user is afforded appropriate access rights to the client and the server. The user may download his or her "user profile" to instantiate a particular desktop representation or other user preference so that the user consistently sees what he or she expects to see when logging on to the client).

As to claim 5, Dutcher discloses an authentication apparatus according to claim 1, wherein each of said plurality of authentication mechanisms has: a storage unit that has registered authentication information of an object of authentication (Dutcher column 17, lines 67: …To support the storage and retrieval of the user profiles from SMB servers…);

and an authentication determination unit which, in a case where entered authentication information of a user has been registered in said storages unit, is for authenticating this object of authentication (Dutcher column 3, lines 16-19: Following successful authentication, a user account is dynamically established at the client by retrieving from the server user information and a set of "group" privileges associated with the authenticated user…).

As to claim 6, Dutcher discloses an authentication apparatus according to claim 1, further having a start-up unit for starting up an authentication mechanism that has been registered as an effective authentication mechanism by said registration unit (Dutcher column 5, lines 8-21: …This action calls a "graphical identification and authorization" module 15 (sometimes referred to as "gina") that controls the logon sequence. This module displays a logon panel display box 17 to the user and prompts for entry of a userid and password. In a known embodiment, the logon panel typically enables the user to logon against an account held at the client machine itself, or to logon against an account held at the NT server. The gina module 15 controls what servers show up in the logon panel dialog box 18. In particular, when the NT client is installed in the network, the system administrator can point the workstation against an NT domain name, and that domain name then shows up as an authentication option. in addition, the administrator of the NT server may configure the server so "trusted" authentication domains are displayed…).

As to claim 7, Dutcher discloses an authentication method of changing over a plurality of authentication mechanisms and performing authentication, comprising: an input step of inputting authentication information of an object of authentication (Dutcher column 5, lines 5-8: In this known technique, a user seeking to be authenticated at the client simultaneously presses the "control", "alt" and "delete" keys of the keyboard to initiate a logon session);

a determination step of determining whether the authentication information that has been input at said input step is that of an object of authentication that is capable of changing over the plurality of authentication mechanisms (Dutcher column 2, lines 55-64: This enables the user to set up his or her own desktop appearance and preferences, irrespective of where in the network the user logs on. The preferences may include a set of access rights vis-a-vis information retrieved from the server. After the user completes his or her work, the dynamically-established user account may be maintained, disabled or deleted from the client);

a display control step of displaying a list of the plurality of authentication mechanisms if it has been determined at said determination step that the object of authentication is one capable of making the changeover (Dutcher column 3, lines 8-15: If desired, the administrator may then apply a discovery "policy" to tailor the way in which a user may access and interact with the discovered information. Then, when a user attempts to logon, the list(s) (as originally compiled or as modified via what the particular discovery policy allows) are presented to the user to enable the user to select the location(s) at which he or she is to be authenticated);

and a registration step of registering, as an effective authentication mechanism, an authentication mechanism that has been selected from the list displayed at said display control step (Dutcher column 3, lines 16-23: Following successful authentication, a user account is dynamically established at the client by retrieving from the server user information and a set of "group" privileges associated with the authenticated user. A local representation of these privileges is then dynamically created on the client, after which the privileges are linked to the user account to make the user a member of the local representation. In this manner, the group information is saved on the local machine and the authenticated user is afforded appropriate access rights to the client and the server. The user may download his or her "user profile" to instantiate a particular desktop representation or other user preference so that the user consistently sees what he or she expects to see when logging on to the client).

As to claim 8, Dutcher discloses an authentication method of changing over a plurality of authentication mechanisms and performing authentication, comprising: an input step of inputting authentication information of an object of authentication (Dutcher column 5, lines 5-8: In this known technique, a user seeking to be authenticated at the client simultaneously presses the "control", "alt" and "delete" keys of the keyboard to initiate a logon session);

a determination step of determining whether the authentication information that has been input at said input step is that of an object of authentication that is capable of changing over the plurality of authentication mechanisms (Dutcher column 2, lines 55-64: This enables the user to set up his or her own desktop appearance and preferences, irrespective of where in the network the user logs on. The preferences may include a set of access rights vis-a-vis information retrieved from the server. After the user completes his or her work, the dynamically-established user account may be maintained, disabled or deleted from the client);

a display control step of displaying a list of the plurality of authentication mechanisms if it has been determined at said determination step that the object of authentication is one capable of making the changeover (Dutcher column 3, lines 8-15: If desired, the administrator may then apply a discovery "policy" to tailor the way in which a user may access and interact with the discovered information. Then, when a user attempts to logon, the list(s) (as originally compiled or as modified via what the particular discovery policy allows) are presented to the user to enable the user to select the location(s) at which he or she is to be authenticated);

a selection step of selecting an authentication mechanism in the list displayed at said display control step (Dutcher column 3, lines 10-15: Then, when a user attempts to logon, the list(s) (as originally compiled or as modified via what the particular discovery policy allows) are presented to the user to enable the user to select the location(s) at which he or she is to be authenticated);

and a registration step of registering the authentication mechanism, which has been selected at said selection step, as an effective authentication mechanism in a case where the authentication mechanism that has been selected at said selection step has registered authentication information input at said input step (Dutcher column 3, lines 16-23: Following successful authentication, a user account is dynamically established at the client by retrieving from the server user information and a set of "group" privileges associated with the authenticated user. A local representation of these privileges is then dynamically created on the client, after which the privileges are linked to the user account to make the user a member of the local representation. In this manner, the group information is saved on the local machine and the authenticated user is afforded appropriate access rights to the client and the server. The user may download his or her "user profile" to instantiate a particular desktop representation or other user preference so that the user consistently sees what he or she expects to see when logging on to the client).

As to claim 11, Dutcher discloses an authentication method according to any one of claim 7, wherein each of said plurality of authentication mechanisms has a storage unit that registers authentication information of an object of authentication (Dutcher column 17, lines 67: …To support the storage and retrieval of the user profiles from SMB servers…),

and said method further has an authentication determination step which, in a case where entered authentication information of an object of authentication has been registered in said storage unit, is a step of authenticating this object of authentication (Dutcher column 3, lines 16-19: Following successful authentication, a user account is dynamically established at the client by retrieving from the server user information and a set of "group" privileges associated with the authenticated user…).

As to claim 12, Dutcher discloses an authentication method according to claim 7, further having a start-up step of starting up an authentication mechanism that has been registered as an effective authentication mechanism at said registration step (Dutcher column 5, lines 8-21: …This action calls a "graphical identification and authorization" module 15 (sometimes referred to as "gina") that controls the logon sequence. This module displays a logon panel display box 17 to the user and prompts for entry of a userid and password. In a known embodiment, the logon panel typically enables the user to logon against an account held at the client machine itself, or to logon against an account held at the NT server. The gina module 15 controls what servers show up in the logon panel dialog box 18. In particular, when the NT client is installed in the network, the system administrator can point the workstation against an NT domain name, and that domain name then shows up as an authentication option. in addition, the administrator of the NT server may configure the server so "trusted" authentication domains are displayed…).

As to claim 13, Dutcher discloses an authentication method comprising: an input step of inputting authentication information of an object of authentication (Dutcher column 5, lines 5-8: In this known technique, a user seeking to be authenticated at the client simultaneously presses the "control", "alt" and "delete" keys of the keyboard to initiate a logon session);

a first authentication step of authenticating whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the first system if authentication succeeds (Dutcher Figure 4);

a second authentication step of authenticating whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the second system if authentication succeeds (Dutcher column 5, lines 22-31: In this known technique, the gina module 15 tightly controls the locations that are available for authentication to include the local NT workstation itself, the remote NT server 12a, and any other servers that are "trusted" by the NT server that the client is configured against. Generally, only these options are shown to the user seeking authentication, and there are no interfaces available to enable the user to be authenticated from non-native server domains. The present invention addresses this problem);

a control step of controlling whether the object of authentication will be managed under management of the first system or under management of the second system (Dutcher column 6, lines 1-12: Thus, according to a primary goal of the present invention, the homogeneous NT client-server environment is uncoupled so that a user of a Windows NT client (by way of example only) may be authenticated by a non-native server. With respect to authentication of the Windows NT client, the client-server environment is "heterogeneous." Authentication at the client gives the user access to resources on the client system, and when this is done via an account definition held at a server, it also gives the user access to resources at the server network via a single logon. The present invention thus enables a user to select a particular location against which he or she desires to be authenticated…);

and a verification step of verifying that authentication of the object of authentication in the second system has succeeded at said second authentication step; wherein if an instruction that shifts the object of authentication from management under the first system to management under the second system has been recognized, said control step controls said first authentication step and said second authentication step, in order to shift the object of authentication from management under the first system to management under the second system, on the condition that the authentication of the object of authentication at said second authentication step has been verified at said verification step (Dutcher column 20, lines 6-49: Determine Type of Authentication Target. Given a domain name, the domain manager must determine its authentication type. Cached names are first examined to see if the domain has previously been identified. If the domain has not been identified, the domain manager queries each domain driver for ownership. If a domain driver claims ownership of the domain, the type is recorded in the cache. The domain name and driver are thus correlated in the cache. Calling Correct Domain Driver. The domain manager, once ascertaining ownership of a domain, will pass requests (such as a request for user authentication) against that domain to the owning domain driver. Issuing Authentication Calls. In the case of non-NT SMB domains, authentication is accomplished with the following: Call NetUseAdd (a Win32 API) to connect to the IPC resource on the authenticating server. This call results in the following SMBs between the client and the server: Negotiate Protocol--determine software levels of both machines. Session Setup and Connect--validate the userid and password against those stored at the server. If the server indicates success, the sequence continues as: Call NetUserGetInfo (a Win32 API) to retrieve user information for extended validation of user logon hours and other elements. This call results in the following SMB between the client and the server: Transact--generic RPC (remote procedure call) exchange…).

As to claim 14, Dutcher discloses an authentication method according to claim 13, wherein said control step controls said first authentication step in such a manner that the object of authentication is excluded from management at said first authentication step in a case where it is verified at said verification step that the object of authentication has been authenticated at said second authentication step (Dutcher column 9, lines 20-26: The policy mechanism thus allows the administrator to populate an individual client's "from" dialog box, to turn off the user's ability to enter a "custom" authentication location from the logon panel, and/or to turn off (or activate) a "Discover" button that enables the user to effect new discovery…).

As to claim 16, Dutcher discloses an authentication apparatus comprising: an input means for inputting authentication information of an object of authentication (Dutcher column 5, lines 5-8: In this known technique, a user seeking to be authenticated at the client simultaneously presses the "control", "alt" and "delete" keys of the keyboard to initiate a logon session);

a first authentication means for authenticating whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input by said input means, and allowing the object of authentication to access the first system if authentication succeeds (Dutcher Figure 4);

a second authentication means for authenticating whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input by said input means, and allowing the object of authentication to access the second system if authentication succeeds (Dutcher column 5, lines 22-31: In this known technique, the gina module 15 tightly controls the locations that are available for authentication to include the local NT workstation itself, the remote NT server 12a, and any other servers that are "trusted" by the NT server that the client is configured against. Generally, only these options are shown to the user seeking authentication, and there are no interfaces available to enable the user to be authenticated from non-native server domains. The present invention addresses this problem);

a control means for controlling whether the object of authentication will be managed under management of the first system or under management of the second system (Dutcher column 6, lines 1-12: Thus, according to a primary goal of the present invention, the homogeneous NT client-server environment is uncoupled so that a user of a Windows NT client (by way of example only) may be authenticated by a non-native server. With respect to authentication of the Windows NT client, the client-server environment is "heterogeneous." Authentication at the client gives the user access to resources on the client system, and when this is done via an account definition held at a server, it also gives the user access to resources at the server network via a single logon. The present invention thus enables a user to select a particular location against which he or she desires to be authenticated…);

and verification means for verifying that authentication of the object of authentication in the second system by said second authentication means has succeeded; wherein if an instruction that shifts the object of authentication from management under the first system to management under the second system has been recognized, said control means controls said first authentication means and said second authentication means, in order to shift the object of authentication from management under the first system to management under the second system, on the condition that the authentication of the object of authentication by said second authentication means has been verified by said verification means (Dutcher column 20, lines 6-49: Determine Type of Authentication Target. Given a domain name, the domain manager must determine its authentication type. Cached names are first examined to see if the domain has previously been identified. If the domain has not been identified, the domain manager queries each domain driver for ownership. If a domain driver claims ownership of the domain, the type is recorded in the cache. The domain name and driver are thus correlated in the cache. Calling Correct Domain Driver. The domain manager, once ascertaining ownership of a domain, will pass requests (such as a request for user authentication) against that domain to the owning domain driver. Issuing Authentication Calls. In the case of non-NT SMB domains, authentication is accomplished with the following: Call NetUseAdd (a Win32 API) to connect to the IPC resource on the authenticating server. This call results in the following SMBs between the client and the server: Negotiate Protocol--determine software levels of both machines. Session Setup and Connect--validate the userid and password against those stored at the server. If the server indicates success, the sequence continues as: Call NetUserGetInfo (a Win32 API) to retrieve user information for extended validation of user logon hours and other elements. This call results in the following SMB between the client and the server: Transact--generic RPC (remote procedure call) exchange…).

As to claim 17, Dutcher discloses an authentication apparatus according to claim 16, wherein said control means controls said first authentication means in such a manner that the object of authentication is excluded from management by said first authentication means in a case where it is verified by said verification means that the object of authentication has been authenticated by said second authentication means (Dutcher column 9, lines 20-26: The policy mechanism thus allows the administrator to populate an individual client's "from" dialog box, to turn off the user's ability to enter a "custom" authentication location from the logon panel, and/or to turn off (or activate) a "Discover" button that enables the user to effect new discovery…).

As to claim 19, Dutcher discloses an authentication program comprising: code for implementing an input step of inputting authentication information of an object of authentication (Dutcher column 5, lines 5-8: In this known technique, a user seeking to be authenticated at the client simultaneously presses the "control", "alt" and "delete" keys of the keyboard to initiate a logon session);

code for implementing a first authentication step of authenticating whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the first system if authentication succeeds (Dutcher Figure 4);

code for implementing a second authentication step of authenticating whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the second system if authentication succeeds (Dutcher column 5, lines 22-31: In this known technique, the gina module 15 tightly controls the locations that are available for authentication to include the local NT workstation itself, the remote NT server 12a, and any other servers that are "trusted" by the NT server that the client is configured against. Generally, only these options are shown to the user seeking authentication, and there are no interfaces available to enable the user to be authenticated from non-native server domains. The present invention addresses this problem);

code for implementing a control step of controlling whether the object of authentication will be managed under management of the first system or under management of the second system; and (Dutcher column 6, lines 1-12: Thus, according to a primary goal of the present invention, the homogeneous NT client-server environment is uncoupled so that a user of a Windows NT client (by way of example only) may be authenticated by a non-native server. With respect to authentication of the Windows NT client, the client-server environment is "heterogeneous." Authentication at the client gives the user access to resources on the client system, and when this is done via an account definition held at a server, it also gives the user access to resources at the server network via a single logon. The present invention thus enables a user to select a particular location against which he or she desires to be authenticated…);

code for implementing a verification step of verifying that authentication of the object of authentication in the second system has succeeded at said second authentication step; wherein if an instruction that shifts the object of authentication from management under the first system to management under the second system has been recognized, said control step controls said first authentication step and said second authentication step, in order to shift the object of authentication from management under the first system to management under the second system, on the condition that the authentication of the object of authentication at said second authentication step has been verified at said verification step (Dutcher column 20, lines 6-49: Determine Type of Authentication Target. Given a domain name, the domain manager must determine its authentication type. Cached names are first examined to see if the domain has previously been identified. If the domain has not been identified, the domain manager queries each domain driver for ownership. If a domain driver claims ownership of the domain, the type is recorded in the cache. The domain name and driver are thus correlated in the cache. Calling Correct Domain Driver. The domain manager, once ascertaining ownership of a domain, will pass requests (such as a request for user authentication) against that domain to the owning domain driver. Issuing Authentication Calls. In the case of non-NT SMB domains, authentication is accomplished with the following: Call NetUseAdd (a Win32 API) to connect to the IPC resource on the authenticating server. This call results in the following SMBs between the client and the server: Negotiate Protocol--determine software levels of both machines. Session Setup and Connect--validate the userid and password against those stored at the server.

If the server indicates success, the sequence continues as: Call NetUserGetInfo (a Win32 API) to retrieve user information for extended validation of user logon hours and other elements. This call results in the following SMB between the client and the server: Transact--generic RPC (remote procedure call) exchange…).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 3, 4, 9, 10, 15, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6021496 (Dutcher) (Applicant's IDS) as applied to claims 1, 7, 13, and 16 above, and in view of US 20020087894 (Foley) (Applicant's IDS).**

As to claim 3, Dutcher discloses an authentication apparatus according to claim 1. Dutcher fails to teach wherein said input unit reads a card on which authentication information of an object of authentication has been recorded and inputs said authentication information.

However, Foley discloses wherein said input unit reads a card on which authentication information of an object of authentication has been recorded and inputs said authentication information (Foley page 4, paragraph 0031: …If the cookie indicates that the user has selected to use the smart card and PIN authentication method (step 209), then a dialog box requesting a smart card and PIN is presented to the user via a web page (step 211)…).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that smart cards were used to carry authentication information (Foley page 4, paragraph 0031: …If the cookie indicates that the user has selected to use the smart card and PIN authentication method (step 209), then a dialog box requesting a smart card and PIN is presented to the user via a web page (step 211)…).

As to claim 4, Dutcher discloses an authentication apparatus according to claim 1. Dutcher fails to teach wherein said input unit inputs the authentication information by using a web browser.

However, Foley teaches wherein said input unit inputs the authentication information by using a web browser (Foley page 4, paragraph 0031: …if the preference set includes information regarding the user's minimum level of security for authentication, the host may request the appropriate authentication information from the user. For example, if the cookie indicates that the user has selected to use the user identification and password authentication method (step 205), then a dialog box requesting a user identification and password is presented to the user via a web page (step 207)…).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that web browsers were used to input authentication information into the system the user is trying to gain access to (Foley page 4, paragraph 0031: …if the preference set includes information regarding the user's minimum level of security for authentication, the host may request the appropriate authentication information from the user. For example, if the cookie indicates that the user has selected to use the user identification and password authentication method (step 205), then a dialog box requesting a user identification and password is presented to the user via a web page (step 207)…).

As to claim 9, Dutcher discloses an authentication method according to claim 7. Dutcher fails to teach wherein a card on which authentication information of an object of authentication has been recorded is read and said authentication information is input at said input step.

However, Foley discloses wherein a card on which authentication information of an object of authentication has been recorded is read and said authentication information is input at said input step (Foley page 4, paragraph 0031: …If the cookie indicates that the user has selected to use the smart card and PIN authentication method (step 209), then a dialog box requesting a smart card and PIN is presented to the user via a web page (step 211)…).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that smart cards were used to carry authentication information (Foley page 4, paragraph 0031: …If the cookie indicates that the user has selected to use the smart card and PIN authentication method (step 209), then a dialog box requesting a smart card and PIN is presented to the user via a web page (step 211)…).

As to claim 10, Dutcher discloses an authentication method according to claim 7. Dutcher fails to teach wherein the authentication information input by a web browser at said input step.

However, Foley discloses wherein the authentication information input by a web browser at said input step (Foley page 4, paragraph 0031: …if the preference set includes information regarding the user's minimum level of security for authentication, the host may request the appropriate authentication information from the user. For example, if the cookie indicates that the user has selected to use the user identification and password authentication method (step 205), then a dialog box requesting a user identification and password is presented to the user via a web page (step 207)…).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that web browsers were used to input authentication information into the system the user is trying to gain access to (Foley page 4, paragraph 0031: …if the preference set includes information regarding the user's minimum level of security for authentication, the host may request the appropriate authentication information from the user. For example, if the cookie indicates that the user has selected to use the user identification and password authentication method (step 205), then a dialog box requesting a user identification and password is presented to the user via a web page (step 207)…).

As to claim 15, Dutcher discloses an authentication method according to claim 13. Dutcher fails to teach wherein said first authentication step authenticates user-level access privilege, and said second authentication step manages administrator-level access privilege.

However, Foley discloses wherein said first authentication step authenticates user-level access privilege, and said second authentication step manages administrator-level access privilege (Foley page 3, paragraph 0026: The system facilitates a user's selection of a method of authentication for access to the restricted service, wherein the restricted service may require a method of authentication in order to gain access to the restricted service (e.g., the system allows the user to submit a level of security for authentication by entry of the selection into the dialog box) (steps 103-105). Alternatively, a host may select the minimum security level for authentication for the particular user based at least partially upon predetermined characteristics…).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that if both a user and a host can select a different level of authentication then the first step could be user-level and the second step could be administrator-level (Foley page 3, paragraph 0026: The system facilitates a user's selection of a method of authentication for access to the restricted service, wherein the restricted service may require a method of authentication in order to gain access to the restricted service (e.g., the system allows the user to submit a level of security for authentication by entry of the selection into the dialog box) (steps 103-105). Alternatively, a host may select the minimum security level for authentication for the particular user based at least partially upon predetermined characteristics…).

As to claim 18, Dutcher discloses an authentication apparatus according to claim 16. Dutcher fails to disclose wherein said first authentication unit authenticates user-level access privilege, and said second authentication unit manages administrator-level access privilege.

However, Foley discloses wherein said first authentication unit authenticates user-level access privilege, and said second authentication unit manages administrator-level access privilege (Foley page 3, paragraph 0026: The system facilitates a user's selection of a method of authentication for access to the restricted service, wherein the restricted service may require a method of authentication in order to gain access to the restricted service (e.g., the system allows the user to submit a level of security for authentication by entry of the selection into the dialog box) (steps 103-105). Alternatively, a host may select the minimum security level for authentication for the particular user based at least partially upon predetermined characteristics…).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that if both a user and a host can select a different level of authentication then the first step could be user-level and the second step could be administrator-level (Foley page 3, paragraph 0026: The system facilitates a user's selection of a method of authentication for access to the restricted service, wherein the restricted service may require a method of authentication in order to gain access to the restricted service (e.g., the system allows the user to submit a level of security for authentication by entry of the selection into the dialog box) (steps 103-105). Alternatively, a host may select the minimum security level for authentication for the particular user based at least partially upon predetermined characteristics…).

Prior Art

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 7305701 is pertinent because it teaches arrangements specifically identify the authentication mechanism/mechanisms, and/or characteristics thereof, that were used in verifying that a user with a unique name is the actual user that the name implies, to subsequently operating security mechanisms. Thus, differentiating user requests based on this additional information provides additional control. US 7251732 is pertinent because it teaches a mechanism that synchronizes passwords maintained for plural domains. A user maintains accounts in two domains. The first and second domains each maintain tables correlating userIDs

with passwords, such that the same user's password can be different in the different domains. A database stores tables that correlate a given user's userID/password combination in the first domain with his corresponding userID/password combination in the second domain. The database is used to sign the user onto one domain when the user is working in the other domain. When the user changes his password in the first domain, the change is reported to the database, so that the database stores the current password. Optionally, the password change may be reported to the second domain, such that the user will have the same password in both domains. US 7216361 is pertinent because it teaches an adaptive multi-tier authentication system provides secondary tiers of authentication which are used only when the user attempts a connection from a new environment. The invention accepts user input such as login attempts and responses to the system's questions. User login information such as IP address, originating phone number, or cookies on the user's machine are obtained for evaluation. User/usage profiles are kept for each user and the user login information is compared to the information from the user/usage profile for the specific user which contains all of the user information that the user used to establish the account and also the usage profile detailing the user's access patterns.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Rebecca L. Pachura whose telephone number is (571) 270-3402. The examiner can normally be reached on Monday-Thursday 7:30 am-6:00 pm est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ramesh Patel can be reached on (571) 272-3688. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Rebecca L Pachura/
/R. L. P./
Examiner, Art Unit 4171

/Ramesh B. Patel/
Supervisory Patent Examiner, Art Unit 4171